Section 7 – TFM Support Activities/Functions

This section provides the following discussions:

- Section 7.1, User and Facility Assistance
- Section 7.2, Disaster Recovery
- Section 7.3, Security
- Section 7.4, System / Network Administration
- Section 7.5, Application Build Process
- Section 7.6, Training.

7.1 User and Facility Assistance

There are three primary sources of information and technical assistance that NAS users and / or facilities use when they experience problems with any TFM operational or system entity. These primary support functions consist of the following:

- ATCSCC Hotline Support. The Command Center Hotline is open Monday through Friday from 7 A.M. until 11:00 P.M. Eastern Time. It provides the first line of user support to internal TFM automation users (i.e., to FAA and US government users). It is managed and staffed by Kenrob and Associates as part of its ATCSCC Support Team effort.
- Volpe Operations Support. Volpe provides second-level user support. ATCSCC Hotline operators, the Tactical Consumer Advocate (TCA), and the ATCSCC Computer Systems Analyst (CSA) often request Volpe Operations Support staff support to resolve ETMS technical problems. Volpe Operations Support provides services on a 24 X 7 basis and is the backup to the ATCSCC Hotline when the Hotline team is not operational. Computer Sciences Corporation (CSC) manages the Volpe Operations Support Team as part of its VNTSC Support effort.
- ATCSCC TCA Support. The TCA provides assistance to all CDM airline users pertaining to TM initiatives and CDM automation. The TCA position is staffed 7 days a week from 7 A.M. to midnight Eastern Time, except on Sunday mornings when it is closed. The ATCSCC NOM provides TCA coverage when the position is not staffed.

Depending on the problem, circumstances and, to some extent, tradition, other resources are available on an itinerant basis. Examples follow, but they are the exception to how help is usually obtained.

- Airlines may call local facilities for local capacity or weather information

- General aviation participants may call their National Business Area Association (NBAA) representative at the Command Center or may call a local facility
- Facilities may call the ATCSCC Hotline, Volpe Operations Support, or the WJHTC on some remote site issues.

This section discusses the three primary means of user support for ETMS and non-ETMS related issues.

7.1.1 ATCSCC Hotline Support

The ATCSCC Hotline provides TFM operations and technical support to FAA facilities and to other government agencies. It has seven dedicated phone lines. One of the lines is reserved for OPSNET issues and the other six are for ETMS related issues. When an incoming call is received and one or more lines are busy, the call rolls over to the first available line. Approximately 95 per cent of the incoming ATCSCC Hotline calls are related to ETMS and the other 5 per cent are related to OPSNET problems. All ETMS and OPSNET calls are logged and tracked to closure.

When the scope or seriousness of a problem needs to be confirmed, the Hotline operators often call specialists at one of 3 centers: Indianapolis (ZID), Chicago (ZAU), or Jacksonville (ZJX). TM specialists in these centers cooperate in verifying reported problems and help determine whether the reported problem is a system-wide problem.

The ATCSCC Hotline Support Team resolves many of the reported problems remotely from the ATCSCC. The types of activities that can be performed remotely include, but are not limited to, the following: running diagnostics, starting/stopping applications, pushing files from one workstation to another, and rebooting workstations. The ATCSCC Hotline Support Team contacts the Volpe Support Team for help with the more complex ETMS technical problems. The ATCSCC Hotline Support Team cannot resolve problems that are software bugs or that require software enhancements. ETMS Program Trouble Reports (PTRs) are submitted for these types of problems. PTRs are handled by application development organizations.

7.1.1.1 ATCSCC Hotline Staffing

Four staff members and a team lead comprise the ATCSCC Hotline Support Team. The Hotline operates five days a week during the busiest shifts. It does not operate during midnight shift and on weekends due to economic considerations related to lower traffic volume and reduced system use during those periods. Because users still experience problems during these off times, Volpe provides backup support when the ATCSCC Hotline is inoperative. Problems are most often reported during these time periods by centers that are hubs for overnight courier services, such as FedEx and UPS (e.g, Memphis and Minneapolis Centers), or that have many international flights that initiate from or traverse its airspace (e.g., Cleveland Center).

7.1.1.2 ATCSCC Hotline Trouble Tickets

ATCSCC Hotline operators log each individual ETMS or OPSNET call, even if several different sites report the same problem. They use an internal ATCSCC Hotline ticketing system for logging. The Hotline Team Lead links duplicate tickets later. The internal ticketing system provides a UNIX based 'Wordpad-like' template with a standard set of fields. Completed templates are stored as flat files on an ATCSCC server that is not directly connected, or visible, to anyone outside of the Kenrob and Associates staff and ATT-220.

Each ticket is numbered for future reference and update. After consultation with the Hotline Lead and/or ATT-220, each ticket is assigned a priority level related to the problem's impact. Updates to the ticket are recorded as they occur. All discussions and actions are logged on the ticket.

The ATCSCC Hotline Team uses a variety of automated scripts to manage, analyze, and reference the trouble tickets. Many scripts are run daily. For example, each day the ATCSCC User Hotline Team Leader uses a script to generate an analysis report of all trouble tickets that were changed during the previous day.

If the ATCSCC Hotline staff cannot resolve a problem because it is caused by a software bug or requires a software enhancement, an ETMS Program Trouble Report (PTR) is submitted through the ETMS Data Defect Tracking System (DDTS). In this case, the ticket is modified to link it to the PTR. The ticket remains "Open" until the PTR is resolved and the fix has been installed in an ETMS release. PTRs are tracked and implemented by the ETMS Build Development organization. See also Section 7.5.1, ETMS Build Cycle.

7.1.1.3 Volume and Types of ATCSCC Hotline Problems

According to the 2002 data collected to-date, the ATCSCC Hotline Support is receiving between 75 and 80 calls per day. These calls result in approximately 120 tickets being generated per month with 75 - 80% of those closed within the same month and, often, within the same call. There is a consistent backlog of about 75 open tickets from month to month. New York (ZNY) and Los Angeles (ZLA) Centers are the most active users.

The most common problems reported to the ATCSCC Hotline operators include:

- ETMS/TSD issues: Times, flights, weather, and/or alerts are not updating on the user's workstation. A hung workstation or ETMS Data Acquisition Communications System (DACS) process can cause this.
- WSD issues: Slow updates are most often reported (there is a lot of lag on this system). Also, the WSD display may not come up. This problem can have a variety of sources including a bad IP address, firewall issues, browser settings, etc.
- OPSNET issues: There are very few OPSNET issues. Most reported problems deal with being unable to enter or send counts and are caused by bad hard drives and Windows-related problems.

Problems with other TFM tools such as FSM and RMT are reported. If the problem is not related to operational setup and interpretation of results, it is handed off to the developing organization, such as Volpe, Kenrob and Associates, or Metron Aviation. These types of problems are not logged into the trouble ticket system.

7.1.2 Volpe Operations Support

The Volpe Operations Support Team provides ETMS technical support and has six dedicated phone lines. When an incoming call is received and one or more lines are busy, the call rolls over to the first available line. Some of the phones have voicemail capability that is activated when no one is available to staff the Hotline. This occurs in rare circumstances such as during fire alarms and drills. The voicemail system is not automatic and must be activated and deactivated manually. The Task Operations Manager must be notified if the voicemail system will be used at the end of the shift or for more than 20 minutes. All customer calls are logged and responded to immediately. Most of the calls are from the ATCSCC Hotline Support Team and TFM remote facilities. The Volpe Hotline staff and Manager coordinate very closely with the ATCSCC Hotline staff throughout the day.

Volpe Operators have years of experience and are often able to answer AT operational questions, in addition to technical questions, when the ATCSCC Hotline is not open. If they cannot answer an operational question, they refer the caller to the appropriate information source.

After thoroughly investigating a problem, a Volpe Operator may discover that it is caused by a software bug or requires a software enhancement. In this case, the Volpe Operator submits an ETMS PTR in conjunction with an ETMS developer. All PTRs are discussed during the regular Thursday technical exchange meetings, and are tracked and managed by the ETMS development organization.

7.1.2.1 Volpe Operations Support Staffing

Volpe Operations Support is continuous throughout the week. There are three shifts per day. The first shift (morning) which is the busiest, particularly on weekdays, usually includes four operators and two senior leads. Two or three operators work the afternoon and midnight shifts. Volpe operators have a wide range of responsibilities, other than Hotline support, and may move about the room, however, the phones are always audible and are picked up as needed.

The Volpe Hotline Operations manager and senior shift leads carry pagers so they can be quickly reached, as required, to solve critical problems.

7.1.2.2 Volpe Hotline Trouble Tickets

Trouble tickets are entered and maintained in the Volpe Data Defect Tracking System (DDTS), which is web-enabled and plugged into an Apache web server. The DDTS is an off-the-shelf application used to track problems from discovery to closure. The Volpe DDTS database is not actively ‘shared’ with other TFM facilities; however, tickets can be accessed via the Apache web server by ATCSCC Hotline support staff at any time.

The Volpe DDTS interface to the 'ticket system' is via a template. The interface, which has been in use for about two years, uses menus to provide specific options that help keep ticket details consistent in content and depth. All actions are recorded in the trouble ticket as they occur.

A ticket's status can be either “Open” or “Closed”. A ticket is closed when the issue is resolved. Most tickets (approximately 80 percent) are resolved and closed during the call or soon thereafter. At each shift change, an “Open” report is generated. The status of open tickets is also reviewed as part of the total system check that is performed every 2 hours.

7.1.2.3 Volume and Types of Volpe Hotline Problems

The Volpe Hotline receives between 5 and 15 calls per shift. About 90 per cent of the calls relate to ETMS support issues. Approximately 5 per cent of the calls are related to the ETMS NORAD feed, which carries a modified ETMS format to NORAD facilities. Other calls concern the Royal Air Force (RAF)/Air Mobility and NADIN feeds, or occasionally Volpe website/data quality issues.

Most calls are from the ATCSCC Hotline staff and from FAA remote facilities. Calls from the FAA remote facilities occur both when the ATCSCC Hotline is open and when it is not open. The remaining calls are from the ATCSCC TCA, WJHTC, the military, and the airlines.

7.1.3 ATCSCC Hotline and Volpe Operations Support Coordination

During times when the ATCSCC Hotline is inoperative, the Volpe Operations Support Team fields, logs, and supports user calls. The Volpe log is accessible via the ETMS WAN and a web browser. The ATCSCC Hotline staff accesses and reviews entries in the Volpe log each morning when their support resumes. Additionally, the ATCSCC Hotline staff generates a summary report of their ticket activity from the day before and sends it to Volpe. The summary includes a short description of the tickets/issues from the previous day and the actions taken or pending. This exchange enables each group to be knowledgeable about all known problems, the actions taken, and what remains to be done.

Each afternoon around 4 P.M., Volpe generates an ETMS ticket summary and sends it to the ATCSCC using ETMS Email. The ATCSCC Hotline Support Team integrates the daily Volpe and ATCSCC ticket summaries together and sends the resulting report to various FAA Headquarters (i.e. to ATT-100) and ATCSCC addresses the next morning.

7.1.4 ATCSCC TCA Support

Refer to Section 4.4.1.7, Tactical Consumer Advocate (TCA), for a discussion of the TCA role.

The TCA deals primarily with CDM participant issues, especially when severe weather limits operations across the NAS. However, the TCA receives calls from other sources, including FAA facilities and, on occasion, the general public. Airlines normally submit their issues by phone but when submitting a specific route request, they may send the request via the ARINC printer.

A large part of the TCA job is coordinating with sectors to address airline requests for exemptions from ongoing TM initiatives. Where necessary the TCA may refer callers directly to the following positions or groups:

- East/West Area for general issues concerning TM initiatives, airport configurations, equipment outages, arrival rates, curfews, etc.
- CSA for technical FSM problems such as substitution errors, ARINC and NADIN issues
- Severe Weather Unit for general routing concerns, NARP/NRP issues, and SWAP issues
- Volpe Hotline or the ATCSCC Hotline as appropriate to the type and level of problem.

7.1.4.1 TCA Staffing

The TCA position is staffed 7 days a week from 7 A.M. to midnight Eastern Time, except on Sunday mornings when it is closed. Currently there are four TCA specialists. Usually one or two TCAs work a shift. Another TCA may be added if there is bad weather. The evening shift is usually the busiest. The NOM assumes the TCA role at midnight.

7.1.4.2 Issue Categories

Normally the TCA deals with issues as they come in. However issues are often sorted into categories to prevent a low priority issue from being handled before a more critical one. Exhibit 7-1. Issue Categories defines the two categories in use.

Exhibit 7-1. Issue Categories

Category 1 Issues	Category 2 Issues
• Unruly passengers, airborne or grounded • Critical loss of crew (loss of crew/aircraft with possible recovery that day) • Fuel critical (possible diversion) • International flight connections • International fuel flight limitations • Fuel critical, unable reroute • No routes available • Airline facility outages (loss of terminal power) • FAA facility outages (services unavailable or restricted) • User gridlock, expected or possible	• Non-critical crew loss (i.e. following day crew rest, replacement crew delay) • Routing questions between SPO TELCONs • Airline/government VIPs, special consideration requests • Sub/SWAP issues (i.e. data problems, reject messages for unknown reasons) • EDCT mismatch (i.e. tower/user times do not match resulting in additional delays)

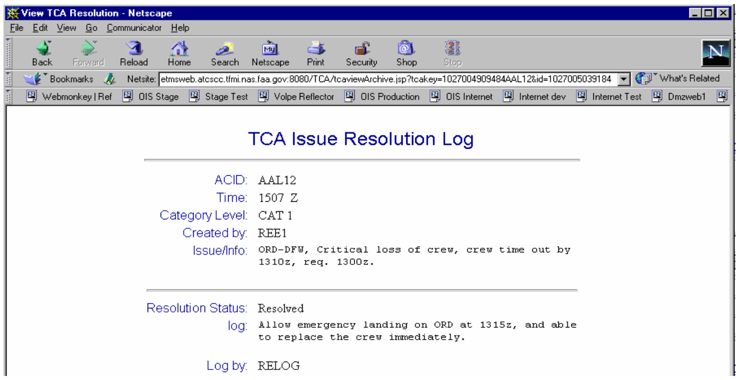
7.1.4.3 TCA Support Process

When severe weather is impacting NAS operations and there is a large volume of incoming calls, the TCA may choose to open up a TCA Hotline. The TCA Hotline is implemented as a TELCON and it replaces individual call answering services. When the Hotline is open, the TCA may make the decision to restrict calls to Category 1 issues.

The TCA informs users of the Hotline start time, the Hotline conferencing number, and the TCA Hotline access number by sending an ETMS general advisory. It is not uncommon for the TCA Hotline support to last four or more hours.

When a TELCON is being used, the procedure is that callers are asked to have all information at hand before calling the TCA Hotline (i.e., call sign, aircraft position, true nature of the problem, alternate route, current EDCT, requested release time, time enroute, etc.). Callers are allowed to submit a maximum of two issues at a time and the TCA keeps a handwritten list of the Hotline issues as the users present them and handles them one-by-one, as soon as feasible.

As of the end of summer 2002, a web-based TCA Tool is available to support the TCA Support function. This tool allows CDM users to enter their issues online. As each issue is handled, the TCA will be able to record his response on the web. This will help reduce redundant questions since all participants will be able to see the answers given to others. See Section 6.2.5.2.12, TCA Tool, for additional information on the TCA Tool. The TCA Tool logs the issues and resolutions. An example of the Issue Resolution Log is shown in Exhibit 7-2. TCA Issue Resolution Log.



TCA Issue Resolution Log

ACID: AAL12
Time: 1507 Z
Category Level: CAT 1
Created by: REE1
Issue/Info: ORD-DFW, Critical loss of crew, crew time out by 1310z, req. 1300z.

Resolution Status: Resolved
log: Allow emergency landing on ORD at 1315z, and able to replace the crew immediately.

Log by: RELOG

Exhibit 7-2. TCA Issue Resolution Log

7.2 Disaster Recovery

This section discusses plans and procedures in place for disaster recovery at the top levels of the TFM domain, where the critical data resides, is developed or tested, is accessed and/or processed for distribution.

Operationally, each remote facility has a Contingency Plan which covers what facility takes over operational TM responsibilities should any local disaster or significant disruption occur. These documents are generally developed locally, in concert with adjacent facilities, and retained at each site. See other sections (such as the Security and Network Administration section, 7.3) for a description of system and network redundancies provided for each remote site facility.

The *ETMS Disaster Recovery Plan* describes the plan for recovery from disasters that may occur at the Volpe Hub site or the ATCSCC.

The following general strategies are currently in place:

- The WJHTC is designated to provide ETMS processing and database backup for the Volpe Hubsite.
- Washington Center (ZDC) maintains an Emergency Operating Facility (EOF) to provide operational backup for the ATCSCC.
- WJHTC is not in the critical operational path and, therefore, no development and testing facility backup is currently assigned for WJHTC.
- Each remote facility has designated one, or more, facilities to take over TM responsibilities. For example, the ATCSCC is the designated operational backup for Oakland Center's (ZOA) oceanic TM functions.

Disaster recovery procedures outlined in this section are also used in the case of general system failures or routine system switchovers at the Hubsite.

7.2.1 ETMS Hub Disaster Recovery

Since ETMS provides the core of TFM functionality, and is a mission-essential system, disaster recovery planning focuses primarily on providing redundancy for the centralized ETMS databases and processing elements at the Volpe Hubsite, and on the networks that provide data between the Hub and remote facilities.

7.2.1.1 First Level of Recovery

The ETMS operational systems at Volpe consist of two duplicate system strings, ETMS A and ETMS B strings. Each of these two strings handles half of the ETMS field sites. They have identical operational databases that are maintained in parallel. Each string, however, has the capacity to handle all the field sites. If either ETMS A or ETMS B fails, the other string takes over the total load and handles all remote field sites. The switchover can be performed in about a minute and the remote sites see no change in operations. A slight slowdown in operations may be experienced but no functionality is lost. Some minimal manual actions are required for the switchover. This recovery process has been tested and is felt to be very reliable as the first line of recovery for a failed ETMS hubsite operational string.

7.2.1.2 Second Level of Recovery

Each ETMS operational string also has a backup string. ETMS A (A01) has a backup string (B10) and ETMS B (B01) has a backup string (A10). If the ETMS A (A01) string experiences a failure and the operational hub is switched over to all remote sites running off the ETMS B (B01) string, the backup ETMS A (B10) string can be brought online in a matter of 20 to 40 minutes such that the operational hub can then be back online with two duplicate systems performing the ETMS hub functions. The process of transferring and checking all data to ensure the backup string has the same operational data as the active string is called a “Cross String Recovery”. The ETMS A (A01) string can be repaired and act as the backup for B10 until such time as operations personnel want to make the switchover back to the original configuration. This recovery process is routinely tested and is felt to be very reliable as the second line of recovery for a failed Hub site operational string. Detailed descriptions of the Cross String Recovery process is described in the Volpe Technical Operations Standard Operating Procedures.

7.2.1.3 Third Level of Recovery

The third level of recovery for ETMS hubsite capabilities assumes a disaster such that the Volpe Center can no longer support the ETMS operations and the activity must be transitioned to the WJHTC. After September 11th, 2001, the WJHTC incorporated two ETMS strings that are 100% dedicated for disaster recovery in case of a complete failure at the Volpe Center. ETMS Strings U and V have been put in place as “hot standbys” at the WJHTC. They contain duplicates of the ETMS operational hub databases and mimic the ETMS A and ETMS B strings. They are not used for any testing activities and are always configured as hot standbys for disaster recovery. The ETMS U and ETMS V strings are connected to a generator and a mini-UPS. If there is a power failure, the mini-UPS will supply the power until the generator takes over.

WJHTC has connectivity to all the remote sites via the Bandwidth Manager. There will be enough bandwidth to support all the sites in an emergency. A Volpe feed (i.e. ETMS A and ETMS B string connections) will be in place by November 2002. WJHTC gets all the raw data that is going to Volpe. WJHTC has direct communication lines to ATCSCC and the alternate ATCSCC.

If a major problem is experienced at the Volpe Center, the operations staff at the ATCSCC and the ETMS field sites become immediately aware that there is a problem and begin analyzing its cause and solution. AUA-700 conducts a telcon among key personnel from AUA-700, the ATCSCC, Volpe, WJHTC and CSC to decide if and when a switchover to the WJHTC should be performed. Once it is decided to perform the switchover, it is estimated to take about 1 hour to complete.

The ATCSCC support staff will make necessary configuration file changes to switch remote site communication lines from Volpe to WJHTC and send them out to the sites. These procedures replace the 1-2 day delay that existed before when building up an operational database for disaster recovery. Now it should take just one hour to switch over to WJHTC as the ETMS operational hub site. This disaster recovery process does allow fallback to Volpe if damage to Volpe is not extensive. A reverse process would be used.

There are however the following ETMS limitations if WJHTC becomes the ETMS hubsite:

- Canada has no physical connection to WJHTC.
- WJHTC does not have VPN applications so Mexico and London will not be connected to WJHTC .
- WJHTC has no connectivity to send data to ASDI vendors.
- WJHTC has no connection to AOCNet or WxNet. Loss of WxNet means no CCFP product at WJHTC.
- WJHTC has link to NADIN, but not ARINC, as its link to ARINC currently is via Volpe.
- Airlines do not have connections to WJHTC's U and V strings so CDM operations will be suspended.
- WJHTC will not be available as a development facility.
- The WJHTC staff needs to be augmented by Volpe staff or others in order to fully support the operational activities of ETMS at WJHTC.

Some other items of note related to redundancy for disaster recovery include the following:

- With each release, the WJHTC provides Volpe with a copy of the remote site source and executables, and Volpe ensures that a copy of the Hubsite executables is available to the WJHTC. Hubsite ETMS source and configuration files, however, are not routinely made available to any other facility at the present time.
- All of the equipment for the ETMS operational hub system is located in the same general physical area within the Volpe Center. Communications lines are divided in half and routed out of opposite sides of the Volpe building.
- Volpe takes backups of operational data every hour, and daily system backups. These backup tapes are stored indefinitely at Volpe, but there is no archive of this data offsite.

The disaster recovery plan for the WJHTC itself addresses the following provisions and constraints:

- While the systems at the WJHTC are contained in a single large room, the layout and protection systems are designed to ensure that the facility remains self-sustaining for short periods of time. A recent trigger of the fire suppression blowout system proved that ETMS equipment would remain operational even if fire suppression chemicals were released.

- An emergency call list has been established for WJHTC. There are a number of cell phones available for calling list members in the event of an emergency.
- There is no backup for the WJHTC. In the event of a long term disaster affecting the WJHTC, partial service can be restored, but, data is an issue since only some data can be regenerated.
- There is no 'autofail rollover' capability at the WJHTC.

7.2.2 ATCSCC Disaster Recovery

The ATC0 Contingency Plan provides for Washington Center (ZDC) to maintain a hot backup for the ATCSCC. The Airspace and Procedures Group maintains the ATC0 Contingency Plan.

ZDC is the disaster recovery site for the ATCSCC. ZDC has active processors that are part of the Emergency Operating Facility (EOF) system providing hot standby for the operational functions of the ATCSCC. These processors are configured for four ATCSCC operational positions, allowing ZDC to assume basic ATCSCC functions for a 'day or two'. A limited number of phone lines, TSDs, and printers are available at ZDC in the EOF. In order for the EOF to provide for ATCSCC responsibilities with regard to issuing GDPs and GSs, the ETMS Autosend function is enabled for the EOF configuration.

In the event of a disaster that necessitates a transfer of ATCSCC functions to the EOF, ATCSCC's hotline support functions would most likely be taken over by Volpe Operations Support, or to a limited degree by the WHJTC.

There is no offsite source protection for code developed at the ATCSCC. All software sources for ATCSCC developed tools are kept on site.

7.3 Security

7.3.1 Overview

This section describes the network infrastructure and application level initiatives that form the basis of the TFM system security. TFM security management responsibilities and the documents that govern TFM security requirements are also outlined in this section.

7.3.2 Security Management

The National Manager of ETMS Operations (ATT-220), an office located at the ATCSCC, manages the ETMS secure infrastructure architecture. The responsibilities of this position include security and network management. The ETMS FAA Security Manager is responsible for the day-to-day management of ETMS security at the ATCSCC and for overseeing security at field sites.

At Volpe, the System Administration staff has responsibility for ETMS security. The focus of security at Volpe is on protection of the Hubsite systems against outside users and pseudo-trusted parties (e.g. ARINC, WxNet).

At the ATCSCC, the ATCSCC Support staff oversees security for the ATCSCC systems and, remotely, for field sites. The focus of security at the ATCSCC is on protecting against other systems and active attacks.

At the WJHTC, the ETMS Group Manager (ACB-750) is responsible for security planning, activities, and systems. Day-to-day security maintenance tasks are currently contracted out to AS&T. WJHTC is not an operational facility but since it is a backup for Volpe, it therefore must maintain security as though it is actively connected to other sites.

ARTCC security is undergoing transition from AUA-700 to the Office of the Assistant Administrator for Information Services & Chief Information Officer (AIO).

7.3.3 Security Documentation

All TFM security is subject first to requirements included in the FAA Information Systems Security Program, FAA Order 1370.82. ETMS and other systems and applications within the TFM-I environment, if they communicate with ETMS in any way, or use the ETMS secure network, must comply with and operate under the security constraints imposed for the ETMS. In addition, any system deemed operationally certified within the TFM domain must adhere to policies and standards noted in this Order.

Interfaces between ETMS and other FAA systems must adhere to the ETMS Security Plan. Security for systems outside the FAA domain that interact with ETMS (such as OAG, WSI and ARINC) must also meet FAA-STD-045 standards. See Section 4.6, TFM Interfaces, for further details about ETMS interfaces.

In addition, all systems within the TFM environment are now subject to the requirements of the TFM-I Information System Security Plan, TMS-SEC-PLN004 V4.1.1, dated 1 June 2002, which identifies the scope of the TFM domain and provides detailed security provisions for:

- Information
- Personnel
- Facilities
- Equipment
- Documentation.

The appendices to the Plan include details about the following: Disaster Recovery Plan, INFOSEC Test and Evaluation Plan, Penetration Test Plan, Penetration Test Results, Hub Physical Security, and Security Procedures. This Plan is updated yearly.

The Enhanced Traffic Management System (ETMS) System Administration Manual (SAM), Version 7.3, for Enhanced Traffic Management System (ETMS) Software Support, CSC/E2-00/7353, also provides information relevant to network administration including ETMS/NAS communications, router and hub management guidelines, and the Host Computer System interface requirements.

7.3.4 Security Approaches

7.3.4.1 Physical Security

Physical and procedural provisions provide much of the access control to the TFM systems at FAA facilities. Users at ATCSCC, Volpe, and field sites must be identified and access to operational areas is controlled.

Access to an operational TMU workstation does not require any login. Login is required for a workstation only if a previous Specialist logs out of a workstation at the end of his shift. No login is required to access the ETMS application and most other TFM tools at the TMU operational area as the ETMS fileservers run continuously and are not logged out. The TMLog tool, however, does require a login.

7.3.4.2 Network Security

The focus of the TFM security is the networks. Each network within the TFM environment is secured through hardware barriers and network administration/software processes and procedures. All the network infrastructures at ATCSCC, Volpe, and WJHTC utilize the same four lines of defense for security provision. These are:

- Routers - Every network within the facility goes through a router with its associated access control lists.

- Firewalls - Part of standard network barrier, firewalls log what messages are blocked and what are passed on the network.
- Intrusion Detection – Intrusion detection systems (IDSs) monitor Internet and Intranet De-Militarized Zones (DMZs), ARINC, ADTN, and WxNet access points as well as production areas against hacking/intrusion.
- 'Humans-in-the-loop' - System administration/support staff at each facility routinely performs security audits on the network. Their duties also include maintaining virus scanning software to the most current levels. Software designs are reviewed for security provisions.

Networks (BWM, CDMNet, AOCNet, WxNet, etc.) and external interfaces (ASDI, ARINC, NADIN, NORAD, etc.) are tightly controlled by routers, firewalls, and IDSs at Volpe, ATCSCC, WJHTC, and the field sites. The details of these TFM network security devices are not available for public release.

Monitor consoles watch the output of intrusion detection systems and any alerts generated are sent to a log that is checked daily. Firewall and router logs are maintained and checked daily. Incident reporting procedures include collecting and retaining hard copies of the above logs.

The Bandwidth Manager (BWM) monitors WAN security.

7.3.4.3 Application Security

At the application level, security is ensured through varied means (access control, password, encryption, etc.). Data from external media are virus scanned every time they are inserted into the TFM environment. This section focuses on major operational applications with the most security concerns/measures: ETMS, the ATCSCC Internet/Intranet websites, the Volpe DataGate Website, TMLog, and WSD. Additional information about the following tools is provided in Section 6, TFM Tools and Products.

ETMS

As ETMS is the most important tool/system within the TFM infrastructure, it contains some comprehensive security features: password protection, access control, encryption, etc.

A hierarchical access control list, which requires passwords, is in place for ETMS across the NAS. Rights and privileges are granted according to job requirements, and usually assigned to groups of staff, as opposed to individuals. System administrators tasked with security tightly control password issuance.

For operational TSD workstations, the password access system is generally transparent to TM specialists. Workstations normally are logged in and run 24 hours a day. Specialists are rarely, if ever, required to log in, since a CSA or other system administration personnel usually logs in a workstation when it is brought online initially. There is no other password access required for running ETMS functions, even for using the ETMS Log capability.

For ETMS system level functions, system administration accounts require passwords, which are controlled by the system administration security manager. All Volpe operations support staff access ETMS using a common password, assigned for their group. System administrators have special privileges such as using Telnet that not permitted for other levels of users. Volpe and ATCSCC support staff have access to unrestricted ETMS Netmail, while other ETMS users have access only to a restricted Netmail command set.

CSAs and other authorized system administration personnel who require root access must currently access it directly using a common password (per site). In order to minimize the number of people who must know this password at any one time and to reduce the need for system administrators to access the root directly, changes are being implemented to support the running of a pseudo program that calls another program as root.

Within ETMS, the File Transfer Program (FTP) and Command Execution (CMD) processes within the ETMS Communications Function provide secure handshaking. This capability requires the use of an encrypted password security table updated monthly at the ATCSCC.

Volpe maintains configuration files that allow identification down to the individual workstation level across the NAS. This structure enables the blocking of ETMS functionality down to the workstation level if required. The configuration files contain the following information: Local site id, site name, node switch socket/mailbox name, remote site id, remote site name, primary server and alternate server IP name and address, client or server designation, polling interval, response time out, size of log/trace file and size of channel queue, and encryption setting.

Data from external media are virus scanned every time they are inserted into the ETMS environment. For example, OAG data is downloaded to a standalone PC, transported to another PC via secure FTP and then manually transferred to ETMS via screened disk media.

Traffic Management Log (TMLog)

Unlike other TFM Tools, the new TMLog tool requires a login password. The functions provided by this tool vary greatly depending on whether one is an administrator, a supervisor, or a specialist, at a field site or at the ATCSCC. The login ID controls the functions available to a user.

ATCSCC Internet/Intranet Websites

Because the ATCSCC Internet site provides applications and information intended for the general public, its access must be open to all. Protection for this site is provided by the ATCSCC infrastructure, i.e. firewalls, DMZ, and IDS. Because the ATCSCC Intranet site provides major tools and information that is limited to the TMUs and CDM participants, its access is controlled and its contents must be protected against inadvertent corruption. The TMUs access the site via direct lines and CDM participant access is protected via passwords and the ETMS network infrastructure.

Volpe DataGate Website

The Volpe DataGate website provides data quality metrics data as well as system and weather status to the CDM participants and FAA Quality Assurance and User Support staff. Users must be registered with Volpe for access to the site. Protection against unauthorized user access is provided by passwords and the ETMS network infrastructure.

Web-based Situation Display (WSD)

WSD provides a TSD-like capability for TRACONs and Towers without an ETMS system. Password authentication is required for access to the WSD application. Three different connections are currently provided for WSD access:

1. ADTN – This connection is designed to serve FAA users at TRACONs and towers where TSDs are not installed. It is accessed via an IP address. ATT-220 is responsible for authorizing users by adding a new user's (static) IP address to the list of authorized users.
2. Internet – This connection is used regularly by approximately 80 military users, based at the Pentagon and on some mobile units (i.e. submarines). Access to WSD via the Internet requires the use of RSA tokens and a pin number. This connection is monitored by an intrusion detection device.
3. Military ACE LAN – This connection serves approximately 7 remote military users at NORAD as well as the West, North and South Air Defense Sectors. As the ACE network is a trusted network, authentication is not required for access from this LAN.

7.4 System/Network Administration

This section describes the TFM system/network administration functions performed at these facilities:

- Volpe
- ATCSCC
- WJHTC
- All other field sites.

In general, system/network administration functions include monitoring and maintenance of operating systems, processors, and networks; network security; and data maintenance. TFM system and network administration tasks are carried out in accordance with procedures outlined in the Enhanced Traffic Management System (ETMS) System Administration Manual (SAM), Version 7.3, for Enhanced Traffic Management System (ETMS) Software Support. CSC/E2-00/7353.

For a description of security initiatives administered by system administration staff at the above facilities, see Section 7.3, Security.

7.4.1 System/Network Administration at Volpe

7.4.1.1 Responsibilities

Volpe system/network administrators are responsible for the monitoring and maintenance of multiple types of operating systems and processors, secure networks, and data feeds that support the hub processing of the TFM system. At Volpe, and at ATCSCC as well, a number of more routine system/network administrative tasks are performed by the Hotline support staff.

System/network administrative tasks include system/network monitoring, data archival, password updating, trouble shooting, and preventative maintenance. Examples of the activities performed at Volpe include:

- Perform full system checks every 2 hours. The purpose of a system check is to ensure that the ETMS is functioning properly such that all necessary data is being received, processed, and transmitted accurately and promptly. All unusual items or events are logged.
- Monitor the FSM/CDM string operations, assessing data quality. Sometimes they switch ADL feeds as required, update the ARINC configuration file as required, and occasionally restart the FSM Manager process.
- Monitor the health of all ETMS remote sites ensuring that the communications nodes are kept fully populated with the latest ETMS version and data (including configuration files).

- Monitor LAN capacities and loading (peak/average) and WAN router loads and performance.
- Periodically perform K-box switch and cross-string switch processes to ensure backups are operating properly.
- Perform manual OAG downloads once a week.
- Monitor the hourly ETMS data archiving process.
- Archive ETMS and FSM data to support trend analysis and debug data (original messages and logs) for operational analysis.
- Perform security password updates whenever a new password file has been generated by the ATCSCC.
- Maintaining the configuration files for both Hubsite server and clients and remote site servers and their clients.

7.4.1.2 Tools

The tools used by System Administrations staff at Volpe include:

- Watchdog - a ‘homegrown’ tool used by ETMS support staff to analyze network timing and efficiency.
- OpenView – used occasionally system-wide on request from the ATCSCC to check on ‘circuits’, to map the WAN for insight as to where the traffic is, or to check on bandwidth utilization. OpenView may also be used in ‘discovery mode’ to see if any illegal LAN connections have been set up at field sites. OpenView is often run in parallel with Watchdog to monitor system health.
- GLANCE PLUS – used for hardware utilization monitoring and for periodic checks on ‘critical systems’.
- ETMS Purger – used to clean out the obsolete data from ETMS every 6 hours.
- NetMetrics – used to analyze maximum and average loads and capacity of the network.
- SAM and STM – HP System Administration toolset and HP Support Tool Manager used for HP maintenance
- CISCO OS Toolset – used for the installation of OS patches and features.
- LINUX OS Toolset - used for the installation of OS patches, system monitoring, and other routine system administration tasks on LINUX systems.
- NT OS Toolset - used for the installation of OS patches, system monitoring, and other routine system administration tasks on Windows NT systems.
- SYSCO Works – used to measure load and performance of the Wide Area Routers and to identify/monitor typical circuits for loads and capacity.
- XSTN – used to check on hardware availability and status.

- ISS Real Source – an Intrusion Detection System used to monitor firewalls/VPN configurations and router logs.
- Telnet – used solely by system administration staff at Volpe and the ATCSCC usually to perform tasks that NetMail is not powerful enough to handle, such as configuring remote site ports.
- UNIX commands and NetMail – used to identify a node that may be malfunctioning and other functions
- ETMS Sup Mode Utility toolset – used to perform many routine ETMS system administration tasks.

7.4.2 System/Network Administration at ATCSCC

7.4.2.1 Responsibilities

Responsibility for the day-to-day management and support of the ATCSCC systems and network rests with the ATCSCC office of the National Manager of ETMS Operations (ATT-220).

The staff providing system support at the ATCSCC includes the system/network administration staff (currently staffed by Kenrob and Associates) and the Computer Systems Analysts (CSAs).

The ATCSCC system/network administrative staff is not only responsible for the system administrative functions at the ATCSCC, but is also responsible for the system administration of the other field sites. Major activities performed by the ATCSCC system/network administration staff include:

- Monitor and maintain the various processors, operating systems, and networks at the ATCSCC. This includes applying operating system patches, monitoring CPU usage and disk utilization, and overseeing the rebooting of the processors periodically.
- Maintain FSM at the ATCSCC. This includes moving FSM files between HP and NT processors and purging obsolete data on a periodic basis. HP systems can use the ETMS Purger utility to purge data but this must be manually initiated on the NT systems.
- Perform incremental, nightly backups and archive operational data from every workstation on the operational floor. The archived data is kept for 15 days.
- Maintain the firewalls, routers, DMZs and other security related equipment and software as well as generate the password security file (used by the ETMS FTP and CMD processes for internal handshaking security) that is sent to Volpe for installation on all nodes.
- For the field site support, monitor the site networks, coordinate system backup and maintenance activities, and resolve any system problems. System problems are often resolved between the ATCSCC Hotline staff and the System Administration staff.

7.4.2.2 Tools

Some of the tools/functions used by system/network administrators at ATCSCC are listed below. Descriptions of most of these tools are already provided earlier in Section 7.4.1, System/Network Administration at Volpe.

- Watchdog
- OpenView
- ETMS Purger
- NetMetrics
- SAM and STM
- CISCO OS Toolset
- LINUX OS Toolset
- NT OS Toolset
- SYSCO Works
- XSTN
- ISS Real Source
- Telnet
- UNIX commands and NetMail.

7.4.2.3 Computer Systems Analyst (CSA) Responsibilities

The Computer Systems Analyst (CSA) at the ATCSCC is the first line of support for the Traffic Management Specialists at the ATCSCC. The CSA desk is located on the operational floor and is usually the first one called upon whenever there is an operational equipment or system problem at the Command Center floor. CSA support is provided from 7 a.m. to 11 p.m., 7 days a week.

The CSAs at the ATCSCC monitor ETMS, remote site connections, data feeds from ARINC, etc. They determine the status of an application, network, workstation, server or other equipment; alert users of an actual or impending system problem; and address any system problem brought up by the Specialists. Much of the CSA job at the ATCSCC is identifying and analyzing program data problems and helping the Specialists with the TFM tools.

7.4.2.4 CSA Tools

Some of the tools (OIS, TSD, etc) used by the CSA are for general situation awareness, while others are used for specific functions performed by the CSA. Some of the applications/tools used at the CSA position include:

- ETMS Log program
- ADL status

- Advisories database list
- OIS
- TSD flight display
- CVRS – used to monitor CVRS heartbeat.
- CDM DataGate website – used to monitor message counts from airlines for continuous spikes which may indicate duplicate data or erroneous feed.
- Watchdog – used to see if remote sites or data feeds are down
- FSM – used to check if any EDCTs or delays are not included when they should have been.
- Replication Monitor Tool – a locally developed tool used for monitoring the three ATCSCC web servers ensure that data is being replicated among them.
- Classview Tool – a locally developed tool that provides an overview of GDP flights.

CSAs at the ATCSCC may also use TM Shell. ETMS Telnet, TSD list request function, ETMS FTP, FTM Connect and NetMail depending on the particular task at hand.

7.4.3 System/Network Administration at WJHTC

7.4.3.1 Responsibilities

Responsibility for day-to-day management of network and system administration functions at the WJHTC is tasked to the ETMS Group Manager, ACB-750. System administration tasks are currently contracted to AS&T.

Since the WJHTC is not an operational site, but is the backup for Volpe, in general, all system and network administration procedures required / performed at Volpe are also performed at the WJHTC, but not on the same schedule as Volpe. Full system checks are done twice a day at WJHTC rather than every 2 hours at Volpe. Firewall and other security logs are maintained and checked every few days as opposed to daily at Volpe.

7.4.3.2 Tools

The tools used for system and network administration functions at WJHTC include:

- OpenView
- HP SAM Toolset
- LINUX OS Toolset
- ETMS Sup Mode Utilities.

7.4.4 System/Network Administration at Other Field Sites

7.4.4.1 Responsibilities

At the remote field sites, the Airway Facilities (AF) staff usually performs routine system/network administration tasks. The local Automation Specialist, who is generally also an active TMC, may perform limited system administration functions, often under the direction of the ATCSCC System Administration staff. The ATCSCC System Administration staff carries out most of the major system administration tasks at the sites remotely.

Within field facilities, there are a number of offices responsible for the maintenance of hardware and software used in the facility, but most of those responsibilities appear to be for the ATC side.

For the TMU area, both AF and TMU personnel take responsibility to monitor the systems and contact appropriate authorities when there are problems. The AF personnel performs routine system and network administration tasks at field facilities according to the schedule outlined in the FAO 6110.11c, Version 4 TMS Maintenance Manual. They do this using provided OS tools and the Sup Mode utilities (executed at a TSD). When they find some element not within tolerances (i.e. CPU or disk space utilization is high), or some hardware equipment not in working order, they notify the TMU Supervisor, Automation Specialist, the ATCSCC Hotline, and/or the hardware contractor as appropriate for the occasion.

Depending on the Automation Specialists, some are able, under the direction of ATCSCC System Administration staff, to perform more complex jobs that are normally done remotely, if there is a need. They follow the ETMS System Administration Manual procedures, just as the AF staff.

Some of the tasks that may be performed by the sites' AF staff and Automation Specialists include:

- Configure and maintain the local network and workstations, monitor processes regularly using NetMail, and/or perform periodic system tasks such as disk cleanup and file maintenance.
- Manage FSM and ETMS server configurations and address any data exchange issues.
- Manage the local Network Information Service (NIS) account functions, i.e. update user accounts and passwords.
- Maintain local configuration files and static adaptation data (thresholds, sector definitions, SDB schedule data).

7.4.4.2 Tools

The following tools may be used at remote site facilities to perform system and network administration tasks:

- ETMS Sup Mode Utilities

- HP SAM and STM tools
- HP IGNITE
- NetMail
- UNIX commands
- LINUX OS Tools
- HP OS Tools
- NT OS Tools.

7.5 Application Build Processes

Nationally deployed TFM Tools described in Section 6.1 are developed and deployed using one of two build cycle process models: the ETMS Build Cycle and the non-ETMS Application Build Cycle. Section 7.5.1 describes the ETMS Build Cycle and Section 7.5.2 describes the non-ETMS Application Build Cycle. ETMS data updating and the INI signoff process are also described in this section.

7.5.1 ETMS Build Cycle

AUA 730 is evolving the ETMS Build Cycle process. The build process in place for ETMS 7.5 development is illustrated in Exhibit 7-3. ETMS Build Cycle. Each build is 8 months long with defined phases, milestones and activities. Build cycles are overlapping so that ETMS builds are released approximately 6 months apart. Each build cycle consists of the following phases:

- Requirements Definition
- Software Development
- System Test
- Acceptance Test
- Operational Test & Evaluation (OT&E)
- Deployment

The above phases are performed by several organizations. During each build cycle, Volpe performs requirements definition, system testing, and acceptance testing; while software development is distributed among several contractors. The FAA at the WJHTC performs Operational Test and Evaluation (OT&E). Volpe, Kenrob and Associates, and Metron Aviation work together to deploy the new ETMS build. Volpe deploys the ETMS Hubsite components, Kenrob and Associates deploys the remote site components, and Metron Aviation deploys FSM to the ATCSCC and the airlines. Each of the ETMS build cycle milestones and activities are discussed below.

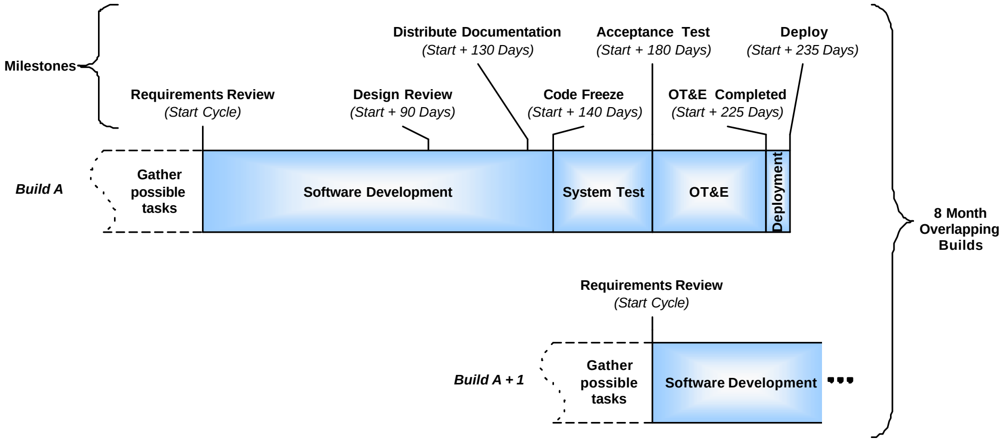


Exhibit 7-3. ETMS Build Cycle

7.5.1.1 ETMS Requirements Definition

Build Functions Identification. Prior to the official start of an ETMS build, the Volpe engineering team identifies potential build functions from a variety of sources. Sources include the list of deferred functions from the previous build, ATT 220 (ETMS Operations) recommended functions, successfully prototyped functions, documented ETMS Engineering Changes (ECs), and CDM Group recommendations. Volpe ensures that all proposed functions are documented as ECs and stored in the ETMS Data Defect Tracking System (DDTS), a commercial Rational tracking tool residing at the William J Hughes Technical Center (WHJTC) in New Jersey. Volpe publishes and distributes the list of proposed build functions to the Build Requirements Review participants prior to the review.

Requirements Review. The Requirements Review functions as a build kickoff. Requirements Review participants include representatives from the FAA (AUA 730), Volpe, the ATCSCC, ATT 220, ETMS software development organizations, ETMS test groups, and ETMS deployment teams. Participants discuss the impacts, alternatives, tradeoffs, priority levels (i.e., High, Medium, and Low), and phasing recommendations for each proposed function. At the conclusion of the review, Volpe prepares and distributes a prioritized list of new requirements to the participants. Functions are classified as *definite* for the upcoming build, *probable* for the upcoming build, *definite* for the subsequent build, and *unallocated*. AUA 730 maintains this list throughout the build.

7.5.1.2 ETMS Software Development

ETMS Software Development begins immediately after the Requirements Review is completed. Activities consist of detailed requirements analysis, design, coding, and software testing by the development organization. The products of this phase include requirements documents and tested code.

Detailed Requirements Analysis. Following the requirements review, Volpe engineers analyze each major build requirement in detail. They evaluate alternatives when necessary, perform tradeoffs between various combinations of requirements and their alternative solutions, determine the "best" build design, and estimate the effort required to develop the selected solutions. Results are documented in two sets of Microsoft Word documents, the *System Requirements* documents and the *Software Requirements* documents. There are separate System Requirements and Software Requirements documents for each build requirement. All requirements are detailed in the System Requirements document, but Software Requirements documents are generated only when requirements do not have a straightforward implementation. All requirements documents are maintained on a Volpe shareable drive that is accessible by all developers and testers.

The *System Requirements* documents provide a high-level view of the new ETMS system functionality. Engineers, developers, and testers contribute to and/or review these documents internally before they are submitted to the FAA for review and approval. The approved documents become part of the ETMS build baseline.

The *Software Requirements* documents are internal documents (i.e., not reviewed/approved by the FAA) that serve as a software design specification for the developers of the new ETMS functionality. These documents include implementation detail. For example, interfaces, dialog boxes, database record definitions, screen layouts and menu options are provided.

In addition to major new functions, each build contains corrections to multiple *Problem Trouble Reports* (PTRs). PTRs are documented and tracked using the ETMS DDTS, which is accessible to all build participants on the ETMS WAN. Refer to Section 7.5.1.7 ETMS Problem Tracking and Management for a description of the PTR handling process. PTRs are reviewed and allocated to builds and software developers on a bi-weekly basis. A separate PTR List is maintained for each build. Because PTRs identify problems with the existing implementation, software developers perform the required analysis. The analysis is documented in DDTS within the PTR record.

Design Review. Volpe hosts the Build Design Review that occurs approximately 3 months after the start of the build. This review is meant to be a follow-up to the Requirements Review that initiated the build. The participants are the same as for the Requirements Review. A high-level system design is presented for some requirements, but not all. The high-level design of those requirements that are being implemented across multiple organizations is presented. Participants also discuss build status and issues so that the FAA can determine if the build is moving in the right direction or if corrective action is needed.

Build requirements and priorities may change as a result of the Design Review. Items may shift among the categories (i.e., definite, probable, etc.), new items may be added to the build requirements list, and additional impacts to requirements changes may be identified. For example, when the requirement for adding beacon codes to the TSD flight data block was discussed, participants realized that applications using the ETMS FTM Connect feature also needed to be changed because the beacon code would be added to the ETMS data transferred through the interface. Participants inform their teams of the changes.

Technical Reviews. In addition to the formal milestone reviews, internal technical reviews occur every six weeks. Engineers, developers, testers, and managers discuss build status and issues. Build requirements and priorities may also change as a result of these reviews. Participants inform their teams of the changes.

Documentation Distribution. The Volpe ETMS Lead Engineer distributes the completed formal System Requirements and Software Requirements documents to build team members via e-mail.

Software Coding and Testing. Coding and unit testing begin as soon as the requirements are understood sufficiently. This often occurs for some of the build functions prior to the formal distribution of the System and Software Requirements documents.

The code and unit test effort is distributed among multiple organizations and locations. There are three major ETMS software development groups: Volpe, CSC, and Metron Aviation. Volpe and its contractors develop the ETMS Hubsite components in Massachusetts on a Development and Test Network that is separate from the ETMS Operational Network located there. CSC and its subcontractors develop the remote site components in New Jersey, and Metron Aviation develops FSM in Virginia. Both CSC and Metron Aviation develop software in their own facilities.

Each organization applies its own software development process and a wide variation in process discipline has been reported. Each organization does use a Configuration Management tool to manage and control source code. Metron Aviation uses Telelogic's Continuous Suite of tools and both Volpe and CSC use Rational ClearCase. Additionally, Volpe and CSC use the same HP compiler versions.

In addition to unit testing, CSC and Metron Aviation perform software integration testing for their assigned components. CSC uses an independent test team from Northrup Grumman during its integration testing.

As an alternative to software integration testing, Volpe uses "early" build testing for the Hubsite components. The System Test Team receives two or three "early" builds, or increments, from the Hubsite development team during the Software Development phase. Each "early" build package contains new and/or revised Hubsite components that have been completed for the build. The test team uses the "early" builds to refine their procedures and to identify integration and other kinds of problems early in the build cycle.

Code Freeze. At the conclusion of the Software Development phase, software code is frozen using Rational ClearCase controls so that changes are controlled during formal testing.

7.5.1.3 ETMS System Testing

System testing begins after the build code freeze and is conducted in accordance with predefined test procedures. Hubsite, remote site, and FSM testing is performed. Additionally, any of the ATCSCC web capabilities (e.g. ADC, RMT, OIS) that are functionally associated with changes to the hub, remote site, or FSM software are also tested.

VolpeTest Configuration. The Volpe test configuration mimics the Hub and 3 remote site configurations (HP, Linux, and an HP/Linux mix). It consists of 2 main HP K Box test strings, Linux, and 4 CDM strings consisting of 2 K Boxes and 2 C Boxes. The K Box strings and Linux are used for Hub and remote site testing, whereas, the CDM strings are used for testing CDM functions such as rerouting and to accommodate airline testing.

The test network has nearly the same live feeds as the operational system. Some of the NAS feeds differ (i.e., ARINC and NADIN data cannot be fed to the test strings due to technical considerations) and, of course, the user driven input differs. The airlines have access to the Volpe Test configuration but, unless system interoperability testing is being performed, there are no live inputs from the airlines. Simulated airline data is currently unavailable although there are plans to develop it in the future. Little, if any, canned data is used because a significant effort is needed to develop the software required to support its use.

The test tools used include:

- XRUNNER helps ensure that all TSD menus, dialog boxes, etc. come up as planned.
- Perl test scripts perform comparisons between test results.
- Purify checks the source code for memory leaks and for pointers and array references that are out of range.
- RAWLOG simulates NAS messages when live data is not used. However, mostly live data is used.
- ClearCase provides configuration management of the build files.
- Local DDTS contains the PTRs detected during the conduct of System and Acceptance Testing. PTRs that are not resolved by the end of Acceptance Testing are moved to the ETMS DDTS.
- ETMS DDTS contains the ECs and PTRs allocated to the build. It resides at the WJHTC and is accessed via the ETMS WAN to access build ECs/PTRs and to input new PTRs after the conclusion of Acceptance Testing.

System Test Preparation. During the software development phase, the ETMS system testers use existing ECs, PTRs, and requirements documents to prepare a set of Microsoft Word-based system test procedures. The System Test Team reviews the procedures internally prior to the start of system testing.

After the software code freeze occurs, executables are created from the configured source code. Volpe creates the Hubsite executables, CSC creates the remote site executables, and Metron Aviation creates the FSM executable. The process for creating these executables is not as straightforward as first imagined due to the following:

- Volpe and CSC are in two distinct geographic locations and each has their own local version of ClearCase. Additionally, some Hubsite components need to execute at the remote sites and some remote site components need to execute at the Hubsite. This means that Volpe and CSC must exchange configured files across the ETMS network before the executables are created.

- Kenrob and Associates and Metron Aviation develop some of the ETMS components needed for the remote sites. Kenrob and Associates and Metron Aviation provide their components to CSC for inclusion in the remote site executable.
- The remote site executable must be supplemented with additional files in order for the build to execute properly at the remote sites. The additional files include adaptation files, configuration files, help files, and scripts. CSC creates a remote site build release package that includes all the necessary files.
- From the perspective of ETMS deployment, the ATCSCC is considered a remote site. From the perspective of FSM, it is different than all other remote sites because it is the only site from which GDPs are issued. Consequently, the FSM interfaces and configuration files for the ATCSCC are different than for other remote sites. FSM at the ATCSCC interfaces with OIS, FSA, and ETMS Autosend / E-mail whereas FSM at other remote sites do not. OIS and FSA are not in the ETMS Test Environment. Additionally, FSM is deployed to the airlines and ETMS is not.

  Because of these FSM characteristics, FSM is handled differently than the other ETMS components. Metron Aviation creates 3 separate FSM installation packages, one each for the ATCSCC, remote sites, and airlines. Each installation package includes the FSM executable and the configuration files it needs to execute in the selected environment. The airline installation package is implemented with Install Shield to simplify installation at non-FAA sites.

Metron Aviation retains the ATCSCC installation package and installs it on the ATCSCC test and training network to permit testing with OIS and FSA. Metron Aviation provides the remote site installation package to CSC who, in turn, includes it in the remote site installation package. Metron Aviation provides the airlines with the airline installation package on CD-ROM if system interoperability testing is planned. CSC provides the remote site installation package to Volpe System Test, WHJTC OT&E, and the ATCSCC deployment team to support their test efforts. Volpe installs the Hubsite and remote site files in the Volpe test environment.

System Test Conduct. Volpe performs all testing prescribed by the System Test Procedures. These include tests for each EC and PTR included in the build as well as installation testing. Rollback procedures are not tested because they do not exist. ETMS has never had to rollback.

The System Test Procedures also include a set of regression tests that evolve from build to build. Since live data is used for regression testing, reports from the test system are compared with reports from the operational system. Comparisons are often automated using scripts or Microsoft Excel functions. The System Test Procedures also contain some load testing whereby load data is compared between the operational and test systems.

When a defect is discovered, the testers generate an internal PTR using a local version of DDTS. Internal PTRs are assigned to developers who make and test the corrections. The updated components are packaged into executables and, for remote site changes, remote site build release packages. The changes are submitted to the Test Team for retest.

System Test is completed when all the system tests have been completed and there are no open Level 1 PTRs against the build. At the conclusion of System Test, a list of all unresolved PTRs against the build is compiled.

Interoperability Testing. Occasionally, build changes have a tremendous impact on the Hubsite components, FSM, and airline flight processing applications. In order to test the interoperability among the disparate processes in a realistic environment, interoperability testing is performed during the System Test timeframe using the Volpe Test configuration, the ATCSCC FSM installation, and live airline data from airlines participating in the test. This testing is *not* a part of formal System Testing. Interoperability tests are *not* defined in the System Test Procedures and system testing can be completed *without* successful completion of the interoperability tests.

Preparation for interoperability testing involves developing an informal test script and coordinating the event with the participants. The test script is loosely defined, often consisting of a timeline of events that need to occur. The script is meant to accommodate ad hoc tests to respond to unexpected situations that occur as the test progresses. One of the test participants agrees to generate the script and distributes it to the other participants. The participants agree on a test date and time.

Interoperability testing is conducted using the Volpe test network and its connections to the ATCSCC and the airlines. Each participant performs their part of the test from their home location. They stay in constant communication via teleconferencing. The participants follow the test script that dictates the sequence of events that occurs among them and their part of the system. The phone is used to communicate the results of each test. Each test participant is free to add in additional tests within the framework of the predefined test script. The test is complete when the script events have been tested and all participants are satisfied.

Interoperability testing was introduced in ETMS 7.4 with the introduction of Simplified Subs. All participants agree that it played an essential role in the test process. It was not used for ETMS 7.5 because the 7.5 changes did not warrant it. It will be considered for subsequent builds.

7.5.1.4 ETMS Acceptance Test

Acceptance testing begins after all of the system tests have been completed. Acceptance test procedures are a subset of the system test procedures that demonstrate major new build capabilities

Acceptance Test Preparation and Conduct. Acceptance testing is a major event lasting two days. Because Acceptance Test Procedures are a subset of the System Test Procedures, Acceptance Testing is more of a demonstration of major new build features than an execution of unique tests. There is a separate test for each major new feature. Acceptance test procedures include the test bed configuration (i.e., which machines are running and what versions of what processes are running on them).

Volpe test team members execute the acceptance tests and representatives from the FAA (AUA 730), WJHTC OT&E, and the ATCSCC witness them. Acceptance Test Procedures are distributed to the attendees one month prior to Acceptance Testing. To date, no requests to modify the procedures have been received from the recipients.

Just as for System Testing, live feeds are used during Acceptance Testing. If comparisons between test and operational system results are outside of expected tolerance levels, the differences must be analyzed and explained and the FAA must accept them as reasonable. There are no hard and fast tolerance levels for differences between the test and operational systems. In some cases, differences are expected due to the build changes. The FAA subjectively determines whether the differences are acceptable based upon the explanation provided.

Defects that are discovered during Acceptance Testing are handled identically to those discovered during System Testing.

Acceptance testing is complete when no Level 1 PTRs are open against the build and OT&E and ATCSCC representatives determine that the build has “passed” Acceptance Testing. In the past, builds have both “failed” and “conditionally passed” Acceptance Testing. Conditional passes are no longer permitted.

At the conclusion of Acceptance testing, new PTRs are generated in the ETMS DDTS for all open PTRs that reside in the local DDTS. The local DDTS PTRs are closed.

7.5.1.5 ETMS OT&E

Operational Test and Evaluation (OT&E) begins after the ETMS build release has passed Acceptance Testing at Volpe. The FAA conducts OT&E at the WJHTC using predefined OT&E Test Procedures.

WJHTC Test Configuration. The WJHTC test lab has a complete set of hardware for the ETMS hub, the ATCSCC, an ARTCC, and a TRACON. Configuration files are modified to mimic any remote site, including the ATCSCC. The lab is set up to test FSM and all three TSD configurations: HP-UX, RedHat Linux, and PCs with the NT Operating System. Plans are underway for developing test beds for non-ETMS applications such as FSA, POET, RMT, and the ATCSCC Intranet web site.

Both live and simulated data feeds are available at the WJHTC, although live data is mostly used. Because WJHTC lacks an ARINC interface, live weather data is accessed via the Volpe data feed. WJHTC does not have a link to the airlines. All airline testing is performed by the CDM participating airlines using their link to the Volpe test string.

The tools used by the OT&E team include the following:

- Toolset Certify (GUI test tool) creates scripts from menu-driven input data. WJHTC currently is migrating from this tool to TestMaster.
- TestMaster reports on the percentage of code undergoing test.

- Word macros are used to test the HCS interface by comparing input stream messages with ETMS internally stored HCS information to ensure that no messages have been lost.
- Excel spreadsheets are set up for each machine to keep track of the directories that are installed on them for each release.
- ClearCase provides configuration management of the build files.
- ETMS DDTS contains the ECs and PTRs allocated to the build. It resides at the WJHTC and is used to retrieve ECs/PTRs being resolved by the build and PTRs detected during Acceptance Testing. New PTRs detected during the conduct of OT&E are also input.

Additionally, the NADIN/ARINC Test Provider tests the NADIN/ARINC interface using an automated tool that provides limited capability only. The tool does not validate the messages that are received.

OT&E Test Preparation. During the Software Development phase, the OT&E staff develops OT&E Test Procedures based on the ECs and PTRs that are allocated to the build and documented in the ETMS DDTS at the WJHTC. OT&E Test Procedures include regression tests and tests for all new and modified build functions. They contain tests to verify the remote site installation scripts as well as Hubsite and remote site rollover and rollback procedures. All OT&E test procedures are documented using Microsoft Word. At one time the OT&E Test Procedures were distributed to Operations staff for external review but no comments were received. Consequently, the test procedures are no longer distributed for review.

After the ETMS Build is accepted, Volpe and CSC rebuild the ETMS executables for OT&E using the same process as they did for System Testing (refer to Section 7.5.1.3 System Testing), however, this time the executables are built from the configured files that were used during Acceptance Testing.

Within a week after the conclusion of Acceptance Testing, the OT&E team receives the configured ClearCase build executables across the ETMS WAN. The test team installs the configured files.

OT&E Test Conduct. The duration of the OT&E phase is six weeks. During this time all the tests in the OT&E Test Procedures document are executed. Complete regression testing usually takes three weeks using 1.5 shifts per day. This includes a minimum of one week to perform stability tests for the Hubsite processing. ATCSCC Operations Support staff participate in the conduct of user-based site testing through a link between the Command Center and the WJHTC Test Lab. Defects that are discovered during OT&E are handled identically to those discovered during System and Acceptance Testing except that PTRs are documented in the ETMS DDTS rather than in the local Volpe DDTS. Refer to Section 7.5.1.7 ETMS Problem Tracking and Management for a description of the PTR handling process.

OT&E is complete at the end of the six-week testing period. At this time, the OT&E Director provides a recommendation to the ETMS Program Office regarding whether the build is ready to be fielded. The recommendation is based upon the number and type of PTRs open at the end of the test period. A minimum criterion for fielding is that there are no open Level 1 PTRs. The Program Office shares the recommendation with ATT 220 (ETMS Operations), and ATT 220 decides if the build is ready for deployment.

7.5.1.6 ETMS Deployment

Since ETMS 7.4, FSM is integrated into ETMS and is deployed at the same time. ETMS/FSM deployment occurs after the successful completion of OT&E. An ETMS/FSM build is deployed in three ways: Volpe deploys the ETMS Hubsite software components onto its own configuration, the Command Center Operations Support staff deploys the ETMS remote site software components to the ATCSCC and other field sites, and Metron Aviation deploys the FSM software to the ATCSCC and the airlines. The ETMS Hubsite and remote site software and FSM software do not always need to be on the same version of the software as long as the software versions are compatible. However, whenever changes to the remote site components or FSM are dependent upon corresponding changes to Hubsite components, deployment among the segments must be coordinated. Volpe performs the coordination.

Deployment Preparation. About one month prior to expected deployment, the ETMS engineers at Volpe begin work on a Deployment Plan. The Deployment Plan defines the deployment strategy and when, and in what order, the Hubsite and remote site components are to be deployed. Depending upon the build, the deployment may occur overnight or may occur in increments over several nights. Deployment activities occur at night when the traffic demand is expected to be very low. The Deployment Plan undergoes limited internal review at Volpe.

At the end of OT&E, configured application files and remote site installation scripts are placed on the Configuration Management (CM) node at the ATCSCC. These files are used for deployment at Volpe and all remote sites.

ATCSCC Deployment Activities. The ATCSCC Operations Support staff performs final testing of the remote site installation scripts. The installation scripts allow build files to be loaded and checked out on the remote site equipment without interfering with the current operational configuration. They contain an array of commands that push out the ETMS build files to multiple sites at once. The installation scripts load the new build files onto remote site equipment but do not start them. The old applications remain running. Use of the installation scripts supports the ETMS deployment goal of making deployment as transparent to the remote sites as possible. Installation scripts are tested using a link to the WJHTC ETMS Test Lab.

Final preparation for remote site deployment involves editing the installation scripts for field implementation, executing the scripts, and checking out the resulting installations. The installation scripts are edited to conform to the desired deployment sequence and to set site-specific values in the ETMS configuration files. Typically, the scripts are set up to push the releases to the field starting with the eastern sites and moving west. The configuration files specify what ETMS functions are enabled at a site. ETMS FTP and ETMS Netmail are used to push the build files to the remote sites using the installation scripts. It usually takes between one and three days to complete this activity with much of the time spent on checkout analysis. For large deployments, it may take as long as one week just to load the software remotely.

Volpe Deployment Activities. While build files are being loaded at the remote sites, a parallel activity occurs at the Hubsite. At the conclusion of OT&E and approximately one week before the build is operationally deployed, the Volpe Operations staff may choose to load the new software onto the Volpe "E" String, a bridge between the test strings and the operational "A" and "B" strings. The new system is "deployment ready" and runs in parallel with the "old" system on the Operational strings. This allows the Volpe Operations staff to monitor the behavior of the new system prior to actual deployment. When the time comes for actual deployment, the Volpe Operational staff may choose to use the E string for a cross string recovery with the first upgraded Hubsite string (either A or B) in order to get the first Hubsite string up and running faster. The remote sites involved in cutover to the new build are connected to the selected system.

Coordinated ATCSCC/Volpe Deployment Activities. After the build files are successfully loaded on both the Hubsite and remote site equipment, actual cutover to the new build occurs at the Hubsite and at the remote sites according to the Volpe Deployment Plan. This ensures that Hubsite and remote site deployment efforts are coordinated. The cutover activities involve the following:

- Ensure the remote site connections to the Volpe Operational strings are consistent with the ETMS deployment strategy. Typically, Hubsite deployment occurs first on one operational string and then on the other. Remote sites that are not being upgraded may need to be connected to the Operational string that is not being upgraded, and the remote sites that are being upgraded may need to be connected to the Operational string selected for upgrade.
- Restart the upgraded ETMS Hubsite processes on the selected operational string.
- Restart the upgraded ETMS processes at the selected remote sites.

Restart of the remote site processes is the only step that is not transparent to the users since their operational processes need to be restarted. The restart can be performed remotely using scripts and ETMS Netmail, or the ATCSCC Operational Support staff may request the System Administrators at the site to restart the process(es). In either case, the remote site System Administrator is already informed about the date and the time of the planned cutover.

After a small checkout period, the remaining Hubsite string and the remote sites connected to it are upgraded using the same cutover process. Provisions are made to accommodate roll back to the previous release for one or more of the new/updated ETMS processes if necessary. Variations of this process do in fact occur. ETMS Hubsite processes may be upgraded incrementally and/or remote site upgrades may be staggered. The variations may occur over the course of one night or may extend over multiple nights.

Metron Aviation Deployment Activities. As discussed in Section 7.5.1.3 System Testing, the FSM interfaces and configuration file settings at the ATCSCC are different than for any other ETMS remote site. Metron Aviation separately installs FSM on each target workstation at the ATCSCC because each of them is configured a little differently than the others and this affects the FSM installation. Installation is performed manually using installation CDs, manual edits of configuration files, and installation scripts.

Metron Aviation sends an installation CD to each of the CDM-participating airlines.

7.5.1.7 ETMS Problem Tracking and Management

ETMS software problems are documented as PTRs residing in the ETMS DDTS at WJHTC. The ETMS DDTS is accessible to all ETMS developers, testers, and users on the ETMS WAN. Anyone can generate a PTR. PTR status/planning meetings are conducted every two weeks via TELCON except during OT&E when they are conducted weekly. Participants include representatives from Volpe, the ETMS software development teams, the ETMS test teams, AUA 730, and the ATCSCC. The ATCSCC establishes the severity level for each new PTR. Severity levels are as follows.

- Level 1 Emergency: A problem exists in the current Operational System and must be fixed and made operational as soon as possible.
- Level 2 Critical: Plan to be fixed in the release in progress. These include minor or rare data loss or corruption problems and crashes unless they are shown to be extremely rare or caused by non-operational procedures.
- Level 3 High: Minor functionality missing. The default category for non-emergency/non-critical.
- Level 4 Medium: Should be fixed but could be fixed after the release is complete (for the next release).
- Level 5 Low: Low level issues to have minimum effect on customer. Coding standard deviations, spelling errors and minor formatting errors that do not affect operation of ETMS belong at this level.

During the PTR meeting, new PTRs are assigned to developers for correction within a specific build. Assignments to developers and builds may be re-evaluated at subsequent PTR meetings when PTR status is provided.

PTR correction is verified during the test process. The tester that verifies the PTR marks it “Verified”. A verified PTR is closed when its associated build is deployed.

The PTR process is documented in the DRAFT General Process for ETMS Software Improvements, Version 2.0, ETMS-SYS-SBP-001.

7.5.1.8 ETMS Configuration Management

ETMS applies configuration management processes to control software, problem reports and system requirements.

All ETMS source, except for FSM, is managed and controlled during software development using Rational’s ClearCase product. It provides version control, check-in/checkout, and merge features. Separate ClearCase libraries are installed at the Volpe and CSC facilities.

FSM source is managed and controlled during software development by Metron Aviation using Telelogic's Continuous tool suite. Its capabilities are similar to ClearCase. Metron Aviation uses Continuous to configure source code, the FSM executable, and the additional files needed to run FSM. From Code Freeze to the end of the ETMS Build Cycle, Metron Aviation provides the current, configured FSM executable, and the files needed to run it, to CSC for inclusion in the remote site build installation package. As such, these files are configured in the ClearCase environment along with the other remote site installation components.

The ATCSCC, through its Kenrob and Associates contractor, controls the official ETMS Configuration Management (CM) library from which ETMS build libraries are distributed. The ETMS CM library is a repository on a workstation at Volpe that is used to store the ETMS software and files that are deployed. The CM library is populated from the ClearCase and Continuous libraries after the conclusion of OT&E.

Software problem reports are maintained and managed using DDTS, a commercial Rational tracking tool. Refer to Section 7.5.1.7 ETMS Problem Tracking and Management for a description of the PTR handling process.

ETMS documentation libraries reside on a file server at Volpe. The server's file management system is used to control access to the libraries. All ETMS developers, testers, and users have access to the file server via the ETMS WAN.

7.5.2 Non-ETMS Application Build Cycle

Non-ETMS traffic management application development is distributed among Volpe, CSC, Kenrob and Associates, and Metron Aviation. Examples of non-ETMS traffic management applications include WSD, the Diversion Recovery Web Page, TMLog, OIS, POET, and RMT. Each application's schedule for the development cycle varies in length and is determined by collaboration between the FAA and the application developer. Generally, application releases are not tied to ETMS releases except when there is a dependency between them and ETMS, as may be case for WSD / CCSD, FSA and others.

The development process discipline varies across development organizations although the standard activities of requirements definition, design, code, test, and deployment are present everywhere. Requirements are gathered from the FAA and application users (e.g., CDM group, QA) and confirmed by the sponsoring FAA organization. They are typically documented and drive subsequent development and test activities. Except for TMLog, independent testing is not performed. FAA Acceptance testing and OT&E[2] are not always performed. Rather prototype systems are fielded at limited sites, comments are collected, and the applications are modified accordingly.

Application source, problem reports, and requirements documentation are configuration managed and controlled using locally maintained flat files. Commercially available configuration management tools are not used. WSD and CCSD appear to be the only

[2] Plans are underway at the WJHTC for developing OT&E test beds for non-ETMS applications that currently are not subjected to OT&E (e.g., FSA, POET, RMT, and the ATCSCC Intranet web site). When the testbed(s) are complete, additional TFM applications will undergo OT&E.

exceptions since problem reports affecting them are stored in the ETMS DDTS because of their close relationship to TSD.

7.5.3 ETMS Data Updates

In between ETMS build releases, there are data updates to ETMS that occur on a regular basis (e.g., 56 day adaptation data update cycle, weekly OAG schedule update cycle). After the data is received at Volpe in accordance with the update schedule, ETMS loads it into the Hubsite computers and extracts, converts, and/or processes the required data to generate ETMS-specific files and databases. The resulting files are shipped to the WJHTC for OT&E testing prior to operational use. See Section 5.3.1 for more information on Operational Data Maintenance.

7.5.4 Inspected Initial Signoff (INI) Process

All applications that are used by FAA Bargaining Unit Employees (BUEs) require NATCA approval before fielding, even if they are prototype systems. ATT 220 (ETMS Operations) is responsible for gaining NATCA approval using the Inspected Initial (INI) signoff process. The approval process occurs when the system under development has stabilized, usually in parallel with the final system test phase of the build cycle. Approval involves a benefits briefing and, sometimes, a demonstration. Once approval is received, the application may be deployed. Training must be provided within 30 days of deployment or the approval is void.

7.6 Training

This section outlines training requirements, courses, responsibilities and systems used to qualify a Traffic Management Specialist for TMU/ATCSCC duties, as well to maintain skills on an ongoing basis. The section is divided into several subsections:

- Entry level Prerequisites
- Basic Training (TMS)
- Other Training
- Ongoing TFM Training
- Training Responsibilities
- Training Schedule
- Training Resources
- Training Equipment.

All training for Traffic Flow Management Specialists is provided in accordance with FAA Order 3120.4J, National Training Order and AEA 7210.34A, Traffic Management Training.

7.6.1 Entry Level Prerequisites

For acceptance as a prospective ATCSCC TM specialist, a minimum of 15 years control experience generally is required, although it is not essential to have had TMC experience in an ARTCC or TRACON prior to moving to the ATCSCC. The ATCSCC tries to select specialists who represent the NAS in terms of east and west operational experience, and level/type of facility (i.e. Center/TRACON).

For ARTCCs, TRACONs, and towers, new TMCs are normally brought in from the floor of their current facility (unless they have TMC experience in another facility and request a transfer).

FAA Academy prepared courses, 50115 and 55116 (Part A- classroom, and Part B – OJT), as described in this section, constitute the formal training program necessary for qualification as a full-performance Traffic Management Specialist.

7.6.2 Basic Training (TMS)

In order to qualify as a TMC in a facility, controllers take several formal courses, beginning with Course 50115 (FAA Academy Training) conducted at the Oklahoma City FAA Training Academy facility and, continuing in the second development phase with Course 55116 (Facility Traffic Management Coordinator) conducted at the trainee's assigned facility. A summary of each of these courses is provided below. Further information about them may be found in FAA Order 3120.4J, Appendix 7.

Additionally, Course 50119 provides ETMS System Administrator training.

Course 50115

Course 50115 is an introductory TFM course delivered at the FAA Academy in Oklahoma City. Fourteen classes are scheduled for 2002, and thirteen for 2003.

Attendees may be fully qualified controllers destined to be TM Specialists, or may be supervisors, staff specialists, personnel required to perform traffic management duties, airway facility (AF/AOS) personnel, and non-FAA participants (domestic and international).

This course takes up to 64 hours to complete, depending on participant needs and class mix. Refer to Exhibit 7-4. Topics Covered in TFM Courses 50115 and 55116 for a summary of the topics that Course 50115 covers in depth.

Exhibit 7-4. Topics Covered in TFM Courses 50115 and 55116

Topics Covered in Course 50115

- The history, present status, and future of the Traffic Management System.
- The documents and operational positions of the Traffic Management Unit. This includes a comprehensive understanding of the equipment used and the functions each system/application is designed to perform for each type of TMS position possible within a facility.
- Traffic Management Workstation and ETMS practical experience in a "hands-on" laboratory environment.
- Procedures used in Severe Weather Management initiatives.
- Procedures for implementing a Ground Delay Program.
- The purpose of and procedures associated with preferred routes, non-preferred routes and the National Route Program (NRP).
- The terms, concepts, and procedures used in TFM initiatives, including the implementation of Departure Sequencing Programs (DSP) and En Route Sequencing Programs (ESP), Arrival Sequencing Programs (Metering) and Tower En Route Control (TEC) service.
- The duties of a Traffic Management Weather Coordinator.
- The duties of a Mission Coordinator.
- The purpose and application of the Traffic Management Contingency Plan and the Contingency Command Post.
- Inter- and intra-facility communications skills practice using scenarios unique to the TFM environment.
- The factors that affect airport capacity and the impact on the National Airspace System

Topics Covered in Course 55116

- The facility Traffic Management mission, an outline of responsibilities and procedures, and the structure of the national TFM system.
- The facility map, common problem areas, and major route structures.
- Site- specific entries for the Traffic Management Workstation including, but not limited to, Traffic Situation Display (TSD), Monitor Alert (MA) and E-mail. This lesson also covers ETMS system administration functions and hardware configurations.
- An introduction to local severe weather management procedures, including such weather sources as FSS, ARTCCs and airlines, SWAP impacts and TM initiatives to address severe weather impacts.
- Site-specific instruction in the development and management of TM initiatives. This includes implementation, monitoring, and revisions for all initiatives/programs affecting departure, en route, and arrival aircraft.
- Preferred routes and the National Route Program (NRP). Preferred and NRP routes, Standard Terminal Arrival (STAR) and Departure Procedure (DP) routes, special flight handling, mission/shuttle launches, and oceanic traffic/routings are discussed.
- The duties, responsibilities, routings and altitudes, coordination, documentation and automation associated with managing Tower En Route Control service(s).
- Basic meteorological systems, associated weather, and the responsibilities and duties of the Weather Coordinator. Weather sources such as NWS, FSS, airlines, ASOS (RVR), LAWRS, TDWR, WARP, CIWS, ITWS may be covered as appropriate to the local facility.
- The duties and responsibilities of the Mission Coordinator position. The types of military airspaces (Air Traffic Control Assigned Airspace (ATCAA), Alert areas, Controlled Firing Area (CFA), Military Operations Area (MOA), Restricted Areas, Warning areas, Prohibited areas) and military routes (IR, VR, SR, AR), and ALTRVs are covered according to need for local/adjacent facility airspaces.
- The role of Traffic Management during emergencies or other unusual situations per the National, Regional and Local Contingency plans in place.
- Miscellaneous local administrative procedures. This may include procedures for opening and closing the TMU/TRACON/sectors, locally required paperwork, KVDT entries, running Data Analysis and Reduction Tool (DART) and National Track Analysis Program (NTAP), use of ATOMS, etc.

The classroom portion of Course 50115 is administered using lesson plans developed by the FAA Academy. Lab training is conducted in a classroom/laboratory environment, utilizing FAA Academy-prepared instructional materials and a synthetic control area.

A multiple-choice test and/or workshop are given at the end of each lesson. In addition, a comprehensive review and multiple-choice test is given at the end of the course. Course 50115 is a pass/fail course for control personnel. TMSIT (Traffic Management Specialists In Training) must achieve a minimum of 70 percent on the end-of-course test to proceed to the next phase of training. For other personnel, course participation is audit only.

Course 55116

Course 55116, conducted at field facilities, is designed primarily for Traffic Management System personnel who have completed course 50115. It is required for position certification at the ATCSCC, level 4 and 5 TRACONs, and ARTCCs. It specifically addresses local policies/directives and procedures. This course is also used to provide refresher training for TM personnel to renew their knowledge of national and local rules and regulations. Portions of this course are sometimes given to TM Specialists who have lost their currency, or who have transferred from another facility.

Course 55116, Part A, supplements and reinforces Course 50115 training and prepares the TMSIT for on-the-job training. Facilities decide which portions of Part A are required based on the needs of the specialist/facility. Refer to Exhibit 7-4. Topics Covered in TFM Courses 50115 and 55116 for a summary of the topics that Course 55116 covers in depth.

The course consists of classroom instruction and on-the-job training (OJT). This training is conducted in a classroom/laboratory environment using an Academy developed outline and facility developed lesson plans, visual aids, and other media designed to support and pace all instruction. Remote facilities (other than the ATCSCC) do not have additional TSD training workstations. Facilities contribute TFM problem scenarios for development of facility specific training objectives.

The course is designed to take a maximum of 80 hours to complete (not including OJT time). Facility training managers determine OJT requirements, in accordance with FAO 3120.4 standards. Guidelines state that OJT should be completed within 10 weeks at ARTCCs and TRACONs and should be completed within 18 weeks at the ATCSCC. Local facilities decide what assessment and completion methodologies and standards to apply.

Course 50119

The FAA Academy also teaches a course for ETMS System Administrators (50119). Six such classes are being conducted in 2002, and four are to be held in 2003. This course is 40 hours long and requires that candidates have TSD operational experience and a working knowledge of UNIX prior to entry.

Course 50119 provides an overview of Traffic Management System hardware and software and addresses specific System Administrator responsibilities. This training is conducted in a classroom/laboratory environment.

CSAs generally attend this course. CSAs usually are the interface between the TMU specialist and Airway Facilities (AF), and are usually the first ones called if there is a problem. CSAs do not have to be TM specialists. However, in some facilities a TM specialist may also perform CSA duties. The CSA at the ATCSCC is not a TM specialist. Contractor system administrators at the WJHTC do not currently attend this course. Contractors are sent to other courses (e.g., Learning Tree) for certification since non-FAA personnel can only audit FAA courses.

The course covers system maintenance and security of the TMS Network and Traffic Management Workstations (TMW) at each field site. Topics include the following:

- Creating servers
- Creating and maintaining the registry
- Customizing the system to user specifications
- Creating backup user files
- Installing new software on the network
- Performing disk cleanup

This material is covered in 18 lessons. The current ETMS documentation set is used as reference material. The course addresses its content through instruction in the following topic areas:

- TMW
- File System Structure
- Editing Text
- Processes
- Basic Commands
- Email/rtr
- Printers
- Backup, Lists, Restore
- Registry
- Directory Structure
- TSD
- Maintenance
- Load Software
- Cron
- Miscellaneous
- Customizing the CDE

7.6.3 Other Training

Course 50113

The ATCSCC is the host (and developer) for the FAA Professional Education Course 50113, National Traffic Management Course. This course is designed primarily for ATC Supervisors in the various FAA radar and tower facilities throughout the country. Other non-ATC FAA as well as airline dispatch and Business Aviation personnel may also participate on a space available basis. The course ran 16 times in FY 2002 from Tuesday through Friday of each scheduled week.

The focus of this course is on understanding the role of traffic management specialists at each type of facility across the NAS, and how traffic management can be applied in a system-wide manner to promote a safe, orderly, economic, and expeditious flow of air traffic. Class members have the opportunity to observe national traffic management operations at the Air Traffic Control System Command Center and to discuss national traffic management initiatives with Air Traffic Control System Command Center personnel.

7.6.4 Ongoing TFM Training

Once a TMC is fully qualified, the types of training received at various times for various purposes may be carried out using any of the following methods:

- Facility Classroom Training
- Cadre Training (‘Train the Trainer’)
- OJT (On the Job Training)
- Monthly Proficiency Training Packages / CBI (Computer Based Instruction)
- Simulation Training (Hands on laboratory training)
- Team Training Meetings and Briefings
- FAM Trips (Familiarization trips)
- Contractor Training Courses (e.g., Metron Aviation for FSM, POET).

Training materials may consist of the following:

- System specific Quick Reference Guides
- Users / Reference Manuals
- Lesson Plans / Course Outlines / Training Workbooks
- Briefing Notes / Guides
- Release Notes
- Online course materials (Metron Aviation)
- CBI disks or videos.

Training Development Responsibility

Volpe currently holds primary responsibility for developing national TFM training course materials, and for release specific training for ETMS and the National TMLog program. Some of this training is delivered via ‘road shows’ or as Cadre training. Some of it is in the form of CBI training, or release notes and local briefings.

Other training is developed and delivered by contractors who may be authorized to provide training while their particular system / application is still in prototype or beta test status. At the present time, even though FSM has been ‘integrated’ into ETMS (at V7.4), Metron Aviation is providing FSM training at their facilities, on-site, or at the ATCSCC (the latter was prior to the events of September 11, 2001; training at the ATCSCC has not yet resumed). Metron’s system training material is also often published on the CDM website.

Not all locally developed TFM tools are well documented, and training for those is informal and done as OJT in most instances.

Computer Based Instruction (CBI)

CBI is used to deliver much of the national, regional and local facility training. CBI courses are developed according to facility, regional or national training directives to cover any subject area, from TFM applications functions, procedures and techniques, communication skills and other human ‘factors’ to equipment operation and maintenance.

All CBI training is implemented in Authorware, is CMI compliant, is designed using a standard Air Traffic navigation template, and runs on a PC platform. Prior to the release of any CBI course, the course is validated to ensure that CBI lessons are technically accurate, meet training requirements, and work as intended. The FAA requires the delivery of the following items prior to the release of any CBI course:

- Application or executable files
- Programming source code
- Copies of electronic clip media files used to assemble the courseware
- Master audio tape used to create audio files
- Training lesson supplements
- Master videotape and any digital video files.

An example of a CBI course offering for more technical personnel is the following, 40-hour, course:

> **#47415, Traffic Flow Management Infrastructure (TFMI)** - This course provides training for technicians, engineers, and FAA Technical Center personnel on ETMS Model HP-C360 equipment. The course is 20 hours self-study text with 20 hours computer-based exercises (CBE). Self-study subjects include system overview,

workstation user environment, UNIX, monitor, keyboard, trackball, tape drive, troubleshooting, and fault isolation procedures. CBE subjects include login, files and directories, basic commands, HP tools, workstation/file-server basics, addresses, diagnostic commands, troubleshooting, and fault isolation.

7.6.5 Training Responsibilities

ATX (ATX-100) is responsible for funding and decision-making regarding FAA Academy training objectives. Facilities and the FAA Academy may identify gaps that require training and submit them for consideration to this authority.

The National Training Manager (ATT-240) oversees ATCSCC and facility TM Specialist training across the NAS. This position is resident at the ATCSCC.

At the ATCSCC, ATT-240 is responsible for ensuring all training records are completed, reviewed and initialed, and that the training room and equipment are maintained in good working condition. ATT-240 maintains OJT records, records of training activity for personnel certified within the previous year, and Form 3120-1 training records. In other facilities, the training specialist/manager assumes these duties.

The STMCs are generally responsible for assigning and overseeing training in their respective areas.

The ATCSCC area specialists are required to provide and receive training as directed by their supervisors.

For each TM specialist, training status/completion is logged no later than 90 days after the month of training completion. Logging occurs in the Training and Proficiency Record, FAA Form 3120 appropriate to the type of facility, or using the TRAX computer program according to the procedures outlined in FAO 3120.4J, Appendix 1.

7.6.6 Training Schedule

An ongoing training program is mandatory for all TM specialists, regardless of facility type. All specialists must complete monthly proficiency CBI course assignments that cover a variety of new and review materials, depending on local facility needs. In addition, training is scheduled for each specialist under the following circumstances:

- Prior to releasing a new operational system, prototype system, or software upgrade
- Prior to implementing a new procedure or significant changes to an existing procedure
- Management determines a need for training or re-training on any system/procedure.

7.6.7 Training Resources

A list of available training is located on the Air Traffic Training web page, which is maintained as part of the FAA Intranet website. The training web page contains a list of national and site specific lessons under development, the CBI national course catalog, forums, and other training information. The website also enables course developers and training site/administrators to find assistance and information required to support their activities and to share information such as FAA-developed/owned graphics, site-developed lessons, or knowledge of active lesson development.

Specialists, managers and training managers have 'hotline' support available to them for CBI hardware and software technical issues and needs, as specified in Chapter 4 of FAO 3120.4J.

7.6.8 Training Equipment/Software

Each facility has a number of PC workstations, usually between ten and twelve, dedicated to CBI training.

CBI training equipment is required to be located in a secure environment, and the CPU is locked when not being accessed by authorized personnel. The hardware and software configurations of the CBI equipment are under national configuration management. Data on the C and E drives are required for the CBI to operate properly. Additions, deletions, or modifications to data on these drives are prohibited without the express written consent of ATX-100 (which is responsible for this equipment).

Some training facilities have training labs where ETMS is installed. The means by which the ETMS training workstations are 'controlled' is via a configuration file maintained at the Hubsite. Each 'site' has a Site ID, Network ID, Process ID, and Node ID. In the case of training positions at the FAA Academy and the ATCSCC, privileges are inhibited at the 'site' level so that no entries can be made which affect live facility operations. Email is usually the only function that is enabled to communicate with other NAS facilities from training positions.

Each facility has a training 'conference' (classroom) room(s) set aside primarily for training use. Training conferences are held frequently throughout the year to ensure that all specialists are up- to-date on system use and procedures.

FAA Academy

The FAA Academy at Oklahoma City has a classroom/laboratory that provides 16-student ETMS/TSD training positions. There are also two additional workstations in that classroom (one is for the instructor and the other is hooked up to an Electrohome/Sony projection screen) and 4 others within the facility (for AVN and system administration purposes). A single PC is attached to the network to enable data transfer to the ETMS workstations using disks.

The current ETMS release is installed at the FAA Academy. The FAA Academy has access to WSD but its operation is not currently a part of the curriculum. ITWS and WARP are not installed at the FAA Academy. Weather data is derived from TSD sources (including CCFP as of V7.4). POET is not available. The FAA Academy does not have DSR or a KVDT for Host interface demonstrations or practice. TMLog runs on 2 workstations for ‘investigation’ purposes only.

Academy positions use live data only at the current time, although they can play back recorded data, and they are experimenting with using historical data (mainly for weather). The issue they are dealing with is that reports are not available for historical data. In short, the training facility has no ‘simulation’ capability for training TM Specialists.

Students at the FAA Academy have access to the ATCSCC Intranet site, OIS and ETMS Email.

ATCSCC

The ATCSCC has a number of ETMS/TSD training positions. These are on a separate ‘site’ (the ATCSCC has four ‘sites’ – FSA, FSB (the operational strings), FSC (testing and training) and FSD (development)). Each ‘site’ has different access privileges depending on its needs. The ATCSCC FSC network is usually connected to the WJHTC ETMSC string. Several layers of configuration files are maintained (at Volpe and at the WJHTC) which block this string from making entries that impact operational ETMS activities across NAS.

Field Sites

Field facilities (ARTCCs/TRACONs/towers) do not have ETMS/TSD workstations dedicated to training. All ETMS training is conducted using operational demonstrations and in the classroom. Classroom training makes use of PowerPoint presentations, CBI, documentation, and other types of media to present “how to” lessons pertaining to TSD and other locally used tools.

This page intentionally left blank